



0460
6-13-01

PATENT #2
81942.0015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

KATAYANAGI, et al.

Serial No: 09/862,888

Filed: May 21, 2001

For: Encryption Method, Decryption Method,
Cryptographic Communication Method,
Cryptographic Communication System,
Memory Product and Data Signal
Embodyed in Carrier Wave

Art Unit: Not Assigned

Examiner: Not Assigned

I hereby certify that this correspondence
is being deposited with the United States
Postal Service with sufficient postage as
first class mail in an envelope addressed
to:

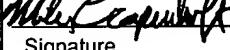
Assistant Commissioner for Patents
Washington D.C. 20231, on

June 18, 2001

Date of Deposit

Michael Crapenhoft, Reg. No. 37,115

Name

 June 18, 2001

Signature

Date

TRANSMITTAL OF PRIORITY DOCUMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

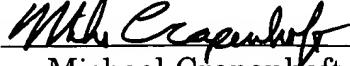
Enclosed herewith is a certified copy of Japanese patent application No. 2001-097701 which was filed March 29, 2001, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: June 18, 2001

By: 
Michael Crapenhoft
Registration No. 37,115
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701



日本特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出願年月日

Date of Application:

2001年 3月29日

出願番号

Application Number:

特願2001-097701

出願人

Applicant(s):

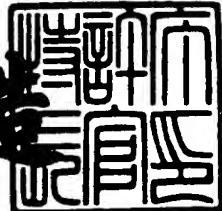
村田機械株式会社
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月11日

特許庁長官
Commissioner,
Japan Patent Office

及川耕



出証番号 出証特2001-3040491

【書類名】 特許願

【整理番号】 21931

【提出日】 平成13年 3月29日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00
H04K 1/00

【発明の名称】 暗号化方法、復号方法、暗号通信方法、暗号通信システム、コンピュータプログラム及び記録媒体

【請求項の数】 30

【発明者】

【住所又は居所】 滋賀県大津市仰木の里東8丁目7-12

【氏名】 片柳 磨子

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町136番地 村田機械株式会社 本社工場内

【氏名】 村上 恭通

【発明者】

【住所又は居所】 大阪府箕面市粟生外院4丁目15番3号

【氏名】 笠原 正雄

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【選任した復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【先の出願に基づく優先権主張】

【出願番号】 特願2000-153358

【出願日】 平成12年 5月 24日

【先の出願に基づく優先権主張】

【出願番号】 特願2000-307822

【出願日】 平成12年10月 6日

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化方法、復号方法、暗号通信方法、暗号通信システム、コンピュータプログラム及び記録媒体

【特許請求の範囲】

【請求項1】 平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルと、公開されている公開ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項2】 前記合成ベクトルの成分と前記公開ベクトルの成分との積和演算結果を法で割った剰余を暗号文とする請求項1に記載の暗号化方法。

【請求項3】 平文から暗号文を得る暗号化方法において、暗号化すべき平文をk分割してなるk個の成分を有する第1ベクトルにn個の任意の乱数を成分とする第2ベクトルを加えた(k+n)個の成分を有する第3ベクトルと、整数 d_i ($1 \leq i \leq k+n$) を用いて (k+n) 個の各成分 D_i が $D_i = d / d_i$ (但し、 $d = d_1 d_2 \cdots d_{k+n}$) に設定された第4ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項4】 平文から暗号文を得る暗号化方法において、暗号化すべき平文をk分割してなるk個の成分を有する第1ベクトルにn個の任意の乱数を成分とする第2ベクトルを加えた(k+n)個の成分を有する第3ベクトルと、整数 d_i ($1 \leq i \leq k+n$) 及び乱数 v_i を用いて (k+n) 個の各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{k+n}$) に設定された第4ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項5】 平文から暗号文を得る暗号化方法において、暗号化すべき平文をk分割してなるk個の成分を有する第1ベクトルにn個の任意の乱数を成分とする第2ベクトルを加えた(k+n)個の成分を有する第3ベクトルと、L組 ($L \geq 2$) の整数 $d_i^{(y)}$ ($1 \leq i \leq k+n, 1 \leq y \leq L$) を用いて各組毎に (k+n) 個の各成分 $D_i^{(y)}$ が $D_i^{(y)} = d^{(y)} / d_i^{(y)}$ (但し、 $d^{(y)} = d_1^{(y)} d_2^{(y)} \cdots d_{k+n}^{(y)}$) に設定されたL組の第4ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項6】 平文から暗号文を得る暗号化方法において、暗号化すべき平文をk分割してなるk個の成分を有する第1ベクトルにn個の任意の乱数を成分とする第2ベクトルを加えた(k+n)個の成分を有する第3ベクトルと、L組(L≥2)の整数 $d_i^{(y)}$ ($1 \leq i \leq k+n$, $1 \leq y \leq L$)及び乱数 $v_i^{(y)}$ を用いて各組毎に(k+n)個の各成分 $v_i^{(y)}$ が $v_i^{(y)} = (d^{(y)} / d_i^{(y)}) \cdot v_i^{(y)}$ (但し、 $d^{(y)} = d_1^{(y)} d_2^{(y)} \cdots d_{k+n}^{(y)}$)に設定されたL組の第4ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項7】 $\text{g c d } (v_i, d_i) = 1$ を満たす請求項4に記載の暗号化方法。

【請求項8】 $\text{g c d } (v_i^{(y)}, d_i^{(y)}) = 1$ を満たす請求項6に記載の暗号化方法。

【請求項9】 $\text{g c d } (d_i^{(y)}, d_j^{(y)}) = 1$ ($1 \leq j \leq k+n$) を満たす請求項6または8に記載の暗号化方法。

【請求項10】 前記第3ベクトルの各成分と、前記第4ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分とによる積和演算に基づいて暗号文を得るようにした請求項3～9の何れかに記載の暗号化方法。

【請求項11】 平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなるk個の成分を有する第1ベクトル、n個の任意の乱数を成分とする第2ベクトル、及び、前記k個の成分または前記n個の成分の位置を特定する情報を示すh個の成分を有する第3ベクトルを加えたK (= k + n + h)個の成分を有する第4ベクトルと、公開されている第5ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項12】 前記暗号文は、前記第4ベクトルと前記第5ベクトルとを用いて得られる複数のブロックから構成されており、各ブロックにおいて、前記第4ベクトルにおける前記h個の成分の位置は同一である請求項11に記載の暗号化方法。

【請求項13】 前記暗号文は、前記第4ベクトルと前記第5ベクトルとを用いて得られる複数のブロックから構成されており、前のブロックでの前記k個の成分に応じて次のブロックでの前記第4ベクトルにおける前記k個の成分また

は前記n個の成分の位置を決定する請求項1-1に記載の暗号化方法。

【請求項1-4】 前記暗号文は、前記第4ベクトルと前記第5ベクトルとを用いて得られる1つのブロックと、前記第3ベクトルのh個の成分を平文を分割してなるh個の成分に置き換えた前記第4ベクトルと前記第5ベクトルとを用いて得られる複数のブロックとから構成されており、前のブロックでの平文を分割してなる前記k個または(k+h)個の成分に応じて次のブロックでの前記第4ベクトルにおける(k+h)個の成分または前記n個の成分の位置を決定する請求項1-1に記載の暗号化方法。

【請求項1-5】 前記第5ベクトルは、整数 d_i ($1 \leq i \leq K$) を用いて各成分 D_i が $D_i = (d / d_i)$ (但し、 $d = d_1 d_2 \dots d_K$) に設定された第6ベクトルとを用いて生成する請求項1-1～1-4の何れかに記載の暗号化方法。

【請求項1-6】 前記第5ベクトルは、整数 d_i ($1 \leq i \leq K$) 及び乱数 v_i を用いて各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \dots d_K$) に設定された第6ベクトルとを用いて生成する請求項1-1～1-4の何れかに記載の暗号化方法。

【請求項1-7】 前記第5ベクトルは、L組 ($L \geq 2$) の整数 $d_i^{(y)}$ ($1 \leq i \leq K$, $1 \leq y \leq L$) を用いて各組毎にK個の各成分 $D_i^{(y)}$ が $D_i^{(y)} = d^{(y)} / d_i^{(y)}$ (但し、 $d^{(y)} = d_1^{(y)} d_2^{(y)} \dots d_K^{(y)}$) に設定されたL組の第6ベクトルとを用いて生成する請求項1-1～1-4の何れかに記載の暗号化方法。

【請求項1-8】 前記第5ベクトルは、L組 ($L \geq 2$) の整数 $d_i^{(y)}$ ($1 \leq i \leq k+n$, $1 \leq y \leq L$) 及び乱数 $v_i^{(y)}$ を用いて各組毎にK個の各成分 $V_i^{(y)}$ が $V_i^{(y)} = (d^{(y)} / d_i^{(y)}) \cdot v_i^{(y)}$ (但し、 $d^{(y)} = d_1^{(y)} d_2^{(y)} \dots d_K^{(y)}$) に設定されたL組の第6ベクトルとを用いて生成する請求項1-1～1-4の何れかに記載の暗号化方法。

【請求項1-9】 $\text{g c d } (V_i, d_i) = 1$ を満たす請求項1-6に記載の暗号化方法。

【請求項2-0】 $\text{g c d } (V_i^{(y)}, d_i^{(y)}) = 1$ を満たす請求項1-8に記載の暗号化方法。

【請求項21】 $\gcd(d_i^{(y)}, d_j^{(y)}) = 1$ ($1 \leq j \leq K$) を満たす請求項18または20に記載の暗号化方法。

【請求項22】 前記第4ベクトルの各成分と、前記第6ベクトルを基にモジュラ変換した前記第5ベクトルの各成分とによる積和演算に基づいて暗号文を得るようにした請求項15～21の何れかに記載の暗号化方法。

【請求項23】 請求項1～10の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記平文ベクトルまたは前記第1ベクトルの成分を、前記乱数ベクトルまたは前記第2ベクトルの成分とは独立的に復号することを特徴とする復号方法。

【請求項24】 請求項1～2または11～21の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記平文ベクトルまたは前記第1ベクトルの成分の位置を同定しながら、前記暗号文を平文に復号することを特徴とする復号方法。

【請求項25】 第1のエンティティ側で、請求項1に記載の暗号化方法に従って平文から暗号文を作成して第2のエンティティ側へ伝送し、伝送された暗号文を該第2のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、前記合成ベクトルにおける前記平文ベクトルの成分または前記乱数ベクトルの成分の位置を前記第1のエンティティ側で設定し、その設定した位置を示す情報を前記第2のエンティティ側へ報知することを特徴とする暗号通信方法。

【請求項26】 前記設定した位置を示す情報を、作成する暗号文に盛り込んで前記第2のエンティティ側へ伝送する請求項25に記載の暗号通信方法。

【請求項27】 第1のエンティティ側で、請求項1に記載の暗号化方法に従って平文から暗号文を作成して第2のエンティティ側へ伝送し、伝送された暗号文を該第2のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、前記合成ベクトルにおける前記平文ベクトルの成分または前記乱数ベクトルの成分の位置を前記第2のエンティティ側で設定し、その設定した位置を示す情報を前記第1のエンティティ側へ報知することを特徴とする暗号通信方法。

【請求項28】 両エンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項1～22の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を第1のエンティティから第2のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備えることを特徴とする暗号通信システム。

【請求項29】 コンピュータに、平文から積和型の暗号文を得ることを実行させるためのコンピュータプログラムにおいて、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えて合成ベクトルを得る手順と、該合成ベクトルと公開されている公開ベクトルとを用いて暗号文を得る手順とを、コンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項30】 コンピュータに、平文から積和型の暗号文を得させるためのコンピュータプログラムを記録してあるコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、該合成ベクトルと公開されている公開ベクトルとを用いて暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系に関し、特に、積和型の暗号文を作成する暗号化方法、その暗号化方法にて得られた暗号文を復号する復号方法、その暗号化方法を利用する暗号通信方法及び暗号通信システム、並びに、その暗号化方法を実施するためのコンピュータプログラム及び記録媒体に関する。

【0002】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」、「マルチアクセス」、「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【0003】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【0004】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者が同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を平文に復号する。

【0005】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵に

よって変換された暗号文は秘密鍵でのみ復号することができる。

【0006】

公開鍵暗号系の1つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をK分割した平文ベクトル $m = (m_1, m_2, \dots, m_K)$ と公開鍵である基底ベクトル $c = (c_1, c_2, \dots, c_K)$ とを用いて、暗号文 $C = m_1 c_1 + m_2 c_2 + \dots + m_K c_K$ を作成し、受信者である他方のエンティティ側でその暗号文Cを秘密鍵を用いて平文ベクトルmに復号して元の平文を得る暗号化方式である。

【0007】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、中国人の剩余定理を用いることにより、高速な並列復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特開2000-89669号）。この暗号化方法は、基底ベクトルcの成分 c_i （ $i = 1, 2, \dots, K$ ）を、互いに素なK個の整数 d_i を用いて $D_i = d / d_i$ （但し、 $d = d_1 d_2 \cdots d_K$ ）に設定した基底 D_i を基にモジュラ変換したもの、または、互いに素なK個の整数 d_i 、乱数 v_i （ $\gcd(d_i, v_i) = 1$ ）を用いて $V_i = (d / d_i) v_i$ に設定した基底 V_i を基にモジュラ変換したものにするなどを特徴としている。このようにして、中国人の剩余定理を用いて並列に復号するので、高速な復号を行うことができる。

【0008】

【発明が解決しようとする課題】

しかしながら、この方式では、公開鍵の数を非常に大きくしない限り低密度であるので、LLL（Lenstra-Lenstra-Lovasz）アルゴリズムを用いて公開鍵と暗号文とから直接平文を求める低密度攻撃に弱い場合があるという問題があり、安全性の面での更なる改良が望まれている。

【0009】

本発明は斯かる事情に鑑みてなされたものであり、上記従来例を改良して低密

度攻撃に強く、安全性を向上できる暗号化方法及び復号方法、この暗号化方法を用いる暗号通信方法及び暗号通信システム、並びに、この暗号化方法をコンピュータに実行させるためのコンピュータプログラム及び記録媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】

請求項1に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルと、公開されている公開ベクトルとを用いて暗号文を得ることを特徴とする。

【0011】

請求項2に係る暗号化方法は、請求項1において、前記合成ベクトルの成分と前記公開ベクトルの成分との積和演算結果を法で割った剰余を暗号文とすることを特徴とする。

【0012】

請求項3に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をk分割してなるk個の成分を有する第1ベクトルにn個の任意の乱数を成分とする第2ベクトルを加えた(k+n)個の成分を有する第3ベクトルと、整数 d_i ($1 \leq i \leq k+n$) を用いて(k+n)個の各成分 D_i が $D_i = d / d_i$ (但し、 $d = d_1 d_2 \cdots d_{k+n}$) に設定された第4ベクトルとを用いて暗号文を得ることを特徴とする。

【0013】

請求項4に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をk分割してなるk個の成分を有する第1ベクトルにn個の任意の乱数を成分とする第2ベクトルを加えた(k+n)個の成分を有する第3ベクトルと、整数 d_i ($1 \leq i \leq k+n$) 及び乱数 v_i を用いて(k+n)個の各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{k+n}$) に設定された第4ベクトルとを用いて暗号文を得ることを特徴とする。

【0014】

請求項5に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をk分割してなるk個の成分を有する第1ベクトルにn個の任意の乱数を成分とする第2ベクトルを加えた(k+n)個の成分を有する第3ベクトルと、L組(L≥2)の整数 $d_i^{(y)}$ (1≤i≤k+n, 1≤y≤L)を用いて各組毎に(k+n)個の各成分 $D_i^{(y)}$ が $D_i^{(y)} = d^{(y)} \neq d_i^{(y)}$ (但し、 $d^{(y)} = d_1^{(y)} d_2^{(y)} \dots d_{k+n}^{(y)}$)に設定されたL組の第4ベクトルとを用いて暗号文を得ることを特徴とする。

【0015】

請求項6に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をk分割してなるk個の成分を有する第1ベクトルにn個の任意の乱数を成分とする第2ベクトルを加えた(k+n)個の成分を有する第3ベクトルと、L組(L≥2)の整数 $d_i^{(y)}$ (1≤i≤k+n, 1≤y≤L)及び乱数 $v_i^{(y)}$ を用いて各組毎に(k+n)個の各成分 $V_i^{(y)}$ が $V_i^{(y)} = (d^{(y)}) \neq d_i^{(y)}$ (但し、 $d^{(y)} = d_1^{(y)} d_2^{(y)} \dots d_{k+n}^{(y)}$)に設定されたL組の第4ベクトルとを用いて暗号文を得ることを特徴とする。

【0016】

請求項7に係る暗号化方法は、請求項4において、 $\text{gcd}(V_i, d_i) = 1$ を満たすことを特徴とする。

【0017】

請求項8に係る暗号化方法は、請求項6において、 $\text{gcd}(V_i^{(y)}, d_i^{(y)}) = 1$ を満たすことを特徴とする。

【0018】

請求項9に係る暗号化方法は、請求項6または8において、 $\text{gcd}(d_i^{(y)}, d_j^{(y)}) = 1$ (1≤j≤k+n)を満たすことを特徴とする。

は8に記載の暗号化方法。

【0019】

請求項10に係る暗号化方法は、請求項3～9の何れかにおいて、前記第3ベクトルの各成分と、前記第4ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分とによる積和演算に基づいて暗号文を得るようにしたことを特徴とする。

【0020】

請求項11に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなるk個の成分を有する第1ベクトル、n個の任意の乱数を成分とする第2ベクトル、及び、前記k個の成分または前記n個の成分の位置を特定する情報を示すh個の成分を有する第3ベクトルを加えたK(=k+n+h)個の成分を有する第4ベクトルと、公開されている第5ベクトルとを用いて暗号文を得ることを特徴とする。

【0021】

請求項12に係る暗号化方法は、請求項11において、前記暗号文は、前記第4ベクトルと前記第5ベクトルとを用いて得られる複数のブロックから構成されており、各ブロックにおいて、前記第4ベクトルにおける前記h個の成分の位置は同一であることを特徴とする。

【0022】

請求項13に係る暗号化方法は、請求項11において、前記暗号文は、前記第4ベクトルと前記第5ベクトルとを用いて得られる複数のブロックから構成されており、前のブロックでの前記k個の成分に応じて次のブロックでの前記第4ベクトルにおける前記k個の成分または前記n個の成分の位置を決定することを特徴とする。

【0023】

請求項14に係る暗号化方法は、請求項11において、前記暗号文は、前記第4ベクトルと前記第5ベクトルとを用いて得られる1つのブロックと、前記第3ベクトルのh個の成分を平文を分割してなるh個の成分に置き換えた前記第4ベクトルと前記第5ベクトルとを用いて得られる複数のブロックとから構成されており、前のブロックでの平文を分割してなる前記k個または(k+h)個の成分に応じて次のブロックでの前記第4ベクトルにおける(k+h)個の成分または前記n個の成分の位置を決定することを特徴とする。

【0024】

請求項15に係る暗号化方法は、請求項11～14の何れかにおいて、前記第5ベクトルは、整数d_i(1≤i≤K)を用いて各成分D_iがD_i=(d/d_i)

) (但し、 $d = d_1 \ d_2 \ \dots \ d_K$) に設定された第6ベクトルとを用いて生成することを特徴とする。

【0025】

請求項16に係る暗号化方法は、請求項11～14の何れかにおいて、前記第5ベクトルは、整数 d_i ($1 \leq i \leq K$) 及び乱数 v_i を用いて各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 \ d_2 \ \dots \ d_K$) に設定された第6ベクトルとを用いて生成することを特徴とする。

【0026】

請求項17に係る暗号化方法は、請求項11～14の何れかにおいて、前記第5ベクトルは、L組 ($L \geq 2$) の整数 $d_i^{(y)}$ ($1 \leq i \leq K, 1 \leq y \leq L$) を用いて各組毎にK個の各成分 $D_i^{(y)}$ が $D_i^{(y)} = d^{(y)} / d_i^{(y)}$ (但し、 $d^{(y)} = d_1^{(y)} \ d_2^{(y)} \ \dots \ d_K^{(y)}$) に設定されたL組の第6ベクトルとを用いて生成することを特徴とする。

【0027】

請求項18に係る暗号化方法は、請求項11～14の何れかにおいて、前記第5ベクトルは、L組 ($L \geq 2$) の整数 $d_i^{(y)}$ ($1 \leq i \leq k+n, 1 \leq y \leq L$) 及び乱数 $v_i^{(y)}$ を用いて各組毎にK個の各成分 $V_i^{(y)}$ が $V_i^{(y)} = (d^{(y)} / d_i^{(y)}) \cdot v_i^{(y)}$ (但し、 $d^{(y)} = d_1^{(y)} \ d_2^{(y)} \ \dots \ d_K^{(y)}$) に設定されたL組の第6ベクトルとを用いて生成することを特徴とする。

【0028】

請求項19に係る暗号化方法は、請求項16において、 $\text{g c d } (V_i, d_i) = 1$ を満たすことを特徴とする。

【0029】

請求項20に係る暗号化方法は、請求項18において、 $\text{g c d } (V_i^{(y)}, d_i^{(y)}) = 1$ を満たすことを特徴とする。

【0030】

請求項21に係る暗号化方法は、請求項18または20において、 $\text{g c d } (d_i^{(y)}, d_j^{(y)}) = 1$ ($1 \leq j \leq K$) を満たすことを特徴とする。

【0031】

請求項22に係る暗号化方法は、請求項15～21の何れかにおいて、前記第4ベクトルの各成分と、前記第6ベクトルを基にモジュラ変換した前記第5ベクトルの各成分による積和演算に基づいて暗号文を得るようにしたことを特徴とする。

【0032】

請求項23に係る復号方法は、請求項1～10の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記平文ベクトルまたは前記第1ベクトルの成分を、前記乱数ベクトルまたは前記第2ベクトルの成分とは独立的に復号することを特徴とする。

【0033】

請求項24に係る復号方法は、請求項1～2または11～21の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記平文ベクトルまたは前記第1ベクトルの成分の位置を同定しながら、前記暗号文を平文に復号することを特徴とする。

【0034】

請求項25に係る暗号通信方法は、第1のエンティティ側で、請求項1に記載の暗号化方法に従って平文から暗号文を作成して第2のエンティティ側へ伝送し、伝送された暗号文を該第2のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、前記合成ベクトルにおける前記平文ベクトルの成分または前記乱数ベクトルの成分の位置を前記第1のエンティティ側で設定し、その設定した位置を示す情報を前記第2のエンティティ側へ報知することを特徴とする。

【0035】

請求項26に係る暗号通信方法は、請求項25において、前記設定した位置を示す情報を、作成する暗号文に盛り込んで前記第2のエンティティ側へ伝送することを特徴とする。

【0036】

請求項27に係る暗号通信方法は、第1のエンティティ側で、請求項1に記載の暗号化方法に従って平文から暗号文を作成して第2のエンティティ側へ伝送し

、伝送された暗号文を該第2のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、前記合成ベクトルにおける前記平文ベクトルの成分または前記乱数ベクトルの成分の位置を前記第2のエンティティ側で設定し、その設定した位置を示す情報を前記第1のエンティティ側へ報知することを特徴とする。

【0037】

請求項28に係る暗号通信システムは、両エンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項1～22の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を第1のエンティティから第2のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備えることを特徴とする。

【0038】

請求項29に係るコンピュータプログラムは、コンピュータに、平文から積和型の暗号文を得ることを実行させるためのコンピュータプログラムにおいて、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えて合成ベクトルを得る手順と、該合成ベクトルと公開されている公開ベクトルとを用いて暗号文を得る手順とを、コンピュータに実行させることを特徴とする。

【0039】

請求項30に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのコンピュータプログラムを記録してあるコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、該合成ベクトルと公開されている公開ベクトルとを用いて暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むコンピュータプログラムを記録してあることを特徴とする。

【0040】

本発明では、平文に冗長性を持たせる、言い換えると平文を退化させて暗号文

を作成する。即ち、暗号化すべき平文を分割してなる平文ベクトルに特に暗号化を必要としない乱数成分からなる乱数ベクトルを付加して合成ベクトルとし、その合成ベクトルと公開されている公開鍵ベクトルとを用いて暗号文を作成する。より具体的には、合成ベクトルの成分と公開ベクトルの成分との積和演算結果、または、その積和演算結果を法で割った剰余を暗号文とする。

【0041】

本発明では、暗号化が必要でない冗長部分（退化部分）を付加しているため、暗号文の密度が高くなり、また、1つの平文ベクトルに対して非常に多数の合成ベクトルつまり非常に多数の暗号文が存在するので、LTLアルゴリズムに基づく低密度攻撃は非常に困難となる。この結果、安全性が向上する。

【0042】

例えば、暗号化すべき平文を分割してなる第1ベクトル（平文ベクトル）及び特に暗号化を必要としない乱数成分からなる第2ベクトル（疑似平文ベクトル）を合わせた第3ベクトル（拡大平文ベクトル）と、各成分を $D_i = d / d_i$ または $V_i = (d / d_i) \cdot v_i$ に設定した1または複数の第4ベクトル（基数ベクトル）とを用いて暗号文を作成する。具体的には、第3ベクトル（拡大平文ベクトル）の各成分と、1または複数の第4ベクトル（基数ベクトル）を基にモジュラ変換した公開鍵ベクトルの各成分との積和演算結果、または、その積和演算結果を法で割った剰余によって暗号文を作成する。

【0043】

また、本来の暗号化すべき平文部分である平文ベクトルの各成分の位置、または、冗長部分（退化部分）である乱数ベクトルの各成分を付加する位置は、固定でなく、送信側のエンティティまたは受信側のエンティティにて任意に設定できる。このように平文部分の位置または冗長部分（退化部分）の付加位置が固定でなく、任意に設定するため、その位置が攻撃者には未知であるため、安全性は更に向かう。

【0044】

また、この設定位置を示す情報は、設定した側のエンティティから他方のエンティティへ、公開で伝えても良いし、秘密裏に伝えても良い。送信側のエンティ

ティがこの位置を設定する場合、その設定位置を示す情報は、暗号文に盛り込んで暗号文と共に受信側のエンティティへ送るようにも良いし、暗号文伝送とは別の経路により受信側のエンティティへ送っても良い。

【0045】

暗号文に盛り込んで設定位置を示す情報を送る場合、具体的には、暗号化すべき平文を分割してなる第1ベクトル（平文ベクトル）、特に暗号化を必要としない乱数成分からなる第2ベクトル（疑似平文ベクトル）、及び、第1ベクトルまたは第2ベクトルの各成分の位置を示す第3ベクトル（位置特定ベクトル）を合わせた第4ベクトル（伸長平文ベクトル）と、公開されている第5ベクトル（公開鍵ベクトル）とを用いて暗号文を作成する。具体的には、第4ベクトル（伸長平文ベクトル）の各成分と、1または複数の第6ベクトル（基数ベクトル）を基にモジュラ変換した第5ベクトル（公開鍵ベクトル）の各成分との積和演算結果、または、その積和演算結果を法で割った剰余によって暗号文を作成する。この際、第3ベクトルの各成分の位置は公開とする。この位置情報は第3ベクトル（位置特定ベクトル）として暗号文に盛り込まれて、受信側のエンティティへ伝送され、その第3ベクトルの各成分の位置は公開されているので、受信側のエンティティにて、第3ベクトルの成分が復号され、その復号結果に基づき第1ベクトル（平文ベクトル）の各成分の位置が分かって、平文に復号できる。

【0046】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図1は、本発明による暗号化方法をエンティティa、b間の情報通信に利用した状態を示す模式図である。図1の例では、一方のエンティティaが、暗号化器1にて平文xを暗号文Cに暗号化し、通信路3を介してその暗号文Cを他方のエンティティbへ送信し、エンティティbが、復号器2にてその暗号文Cを元の平文xに復号する場合を示している。

【0047】

（第1実施の形態）

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵： $\{d_i\}$, $\{d_i'\}$, $\{v_i\}$, P , w

・公開鍵： $\{c_i\}$

【0048】

$e > e'$ として、正規基數 d_i 及び退化基數 d_i' は、夫々下記 (1), (2) を満たす基數と定義する。

【0049】

【数1】

$$d_i = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \quad \dots \quad (1)$$

$$d_i' = 2^{e'} + \delta_i' \quad (1 \ll \delta_i' \ll 2^{e'}) \quad \dots \quad (2)$$

【0050】

$(k+n)$ 個の互いに素な数からなる基數を定める。但し、そのうちの $i \in I$ に対応する k 個を正規基數、 $i \in I'$ に対応する n 個を退化基數とする。ここで、 I, I' は何れもインデックス集合であり、 $I = \{1, 2, \dots, k\}$, $I' = \{k+1, k+2, \dots, k+n\}$ とし、 $I'' = I \cup I'$ とする。なお、第1, 第2実施の形態では、特に断らない限り、 $i \in I''$ である。次に、基數積 D_i を下記 (3) に従って求める。

【0051】

【数2】

$$D_i = \begin{cases} \frac{d_1 \cdots d_k d_{k+1}' \cdots d_{k+n}'}{d_i} & (i \in I) \\ \frac{d_1 \cdots d_k d_{k+1} \cdots d_{k+n}}{d_i} & (i \in I') \end{cases} \quad \dots \quad (3)$$

【0052】

また、 $(k+n)$ 個の乱数 $\{v_i\}$ (但し、 $\gcd(d_i, v_i) = 1$) を生成し、変換基數積 V_i を下記 (4) により導く。

$$V_i = D_i v_i \quad \cdots (4)$$

【0053】

エンティティ a 側で、エンティティ b へ暗号化して送信すべき平文 x を k 分割して、各成分が e (ビット) である平文ベクトル $g = (g_1, g_2, \dots, g_k)$ を得る。また、エンティティ b へ特に送信する必要がない各成分が e (ビット) の乱数からなる疑似平文ベクトル $g' = (g_{k+1}, g_{k+2}, \dots, g_{k+n})$ を得る。例えば、エンティティ b へ特に送信する必要がない平文 (冗長文) を n 分割して、この疑似平文ベクトル g' を得ることができる。これらの平文ベクトル g と疑似平文ベクトル g' とを結合して、(k + n) 個の成分を有する拡大平文ベクトル $g'' = (g_1'', g_2'', \dots, g_{k+n}'')$ を得る。ここで、この拡大平文ベクトル g'' の各成分は、下記 (5) のように定義される。

【0054】

【数3】

$$g''_i = \begin{cases} g_i & (i \in I) \\ g'_i & (i \in I') \end{cases} \quad \cdots (5)$$

【0055】

積和平文 M を、拡大平文ベクトル g'' と変換基數積 V_i とを用いて、下記 (6) のように定義する。

$$M = g_1'' V_1 + g_2'' V_2 + \dots + g_{k+n}'' V_{k+n} \quad \cdots (6)$$

【0056】

任意の拡大平文ベクトル g'' に対して、 $M < P$ を満たす素数 P を生成して法とする。素数 P より小さい乱数 w を定め、下記 (7) に従って、下記 (8) に示すような公開鍵ベクトル c を導いて公開する。

$$c_i \equiv w V_i \pmod{P} \quad \cdots (7)$$

$$\text{ベクトル } c = (c_1, c_2, \dots, c_{k+n}) \quad \cdots (8)$$

【0057】

エンティティ a 側で、拡大平文ベクトル g'' と公開鍵ベクトル c との内積を下

記(9)のように求めて、暗号文Cを得る。作成された暗号文Cは通信路3を介してエンティティaからエンティティbへ送信される。

$$C = g_1'' c_1 + g_2'' c_2 + \cdots + g_{k+n}'' c_{k+n} \quad \cdots (9)$$

【0058】

エンティティb側では、以下のようにして復号処理が行われる。

暗号文Cから積和平文Mは、下記(10)のようにして求めることができる。

$$M \equiv w^{-1} C \pmod{P} \quad \cdots (10)$$

【0059】

拡大平文ベクトル g'' のうち、正規基数に対応するインデックス、即ち、 $i \in I$ に関しては、下記(11)が成立して、平文ベクトル g を復号することができる

$$g_i \equiv M V_i^{-1} \pmod{d_i} \quad \cdots (11)$$

【0060】

なお、退化基数に対応するインデックス、即ち、 $i \in I'$ に関しては、復号する必要がない。また、上記(11)と同様に下記(12)に従って復号しようとしても、退化の影響によりビット数に関して下記(13)の関係があるので、疑似平文ベクトル g' を正しく復号することはできない。

$$g_i''' \equiv M V_i^{-1} \pmod{d_i'} \quad \cdots (12)$$

$$g_i' > d_i' > g_i''' \quad \cdots (13)$$

【0061】

なお、上記例では、 $\text{gcd}(V_i, d_i) = 1$ としたが、 $\text{gcd}(V_i, d_i) = A_i$ としても良い。この場合には、 $V_i' = V_i / A_i$, $d_i' = d_i / A_i$ とおいて、 $\text{gcd}(V_i', d_i') = 1$ として同様に行けば良い。また、上記例では、基數積 D_i に乱数 $\{v_i\}$ を付加するようにしたが、このような乱数を付加せず、上記(3)で示される基數積 D_i をそのまま用いても良い。

【0062】

(第2実施の形態)

秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵： $\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$, $\{d_i^{(P)'}\}$, $\{d_i^{(Q)'}\}$,

$\{v_i^{(P)}\}$, $\{v_i^{(Q)}\}$, P, Q, N, w

・公開鍵: $\{c_i\}$

なお、上記Nは公開であっても良い。

【0063】

P, Q を後述の条件を満たす素数とする。 $e > e'$ とし、正規基數 $d_i^{(P)}$, $d_i^{(Q)}$ 及び退化基數 $d_i^{(P)'} , d_i^{(Q)'}$ は、夫々下記 (14), (15) を満たす基數と定義する。

【0064】

【数4】

$$d_i^{(P)} d_i^{(Q)} = 2^e + \delta ; \quad (1 \ll \delta ; \ll 2^e) \dots (14)$$

$$d_i^{(P)'} d_i^{(Q)'} = 2^{e'} + \delta' ; \quad (1 \ll \delta' \ll 2^{e'}) \dots (15)$$

【0065】

法P及び法Qについて、夫々第1実施の形態と同様に、2組の基數 $\{d_i^{(P)}\}$, $\{d_i^{(P)'}\}$ 及び $\{d_i^{(Q)}\}$, $\{d_i^{(Q)'}\}$ (但し、 $i \neq j$ において、 $\gcd(d_i^{(P)}, d_j^{(P)}) = 1$, $\gcd(d_i^{(Q)}, d_j^{(Q)}) = 1$) を生成する。但し、任意の $i \in I''$ について、下記 (16), (17) を満たすものとする。

$$\gcd(d_i^{(P)}, d_i^{(Q)}) = 1 \dots (16)$$

$$\gcd(d_i^{(P)'}, d_i^{(Q)'}) = 1 \dots (17)$$

【0066】

次に、法P及び法Qについて、第1実施の形態と同様に、2組の乱数 $\{v_i^{(P)}\}$ 及び $\{v_i^{(Q)}\}$ (但し、 $\gcd(d_i^{(P)}, v_i^{(P)}) = 1$, $\gcd(d_i^{(Q)}, v_i^{(Q)}) = 1$) を生成し、上記 (3), (4) と同様の計算により、 $\{V_i^{(P)}\}$ 及び $\{V_i^{(Q)}\}$ を導く。

【0067】

第1実施の形態と全く同様に構成された拡大平文ベクトル g'' に対する法P及び法Qにおける積和平文 M_P 及び積和平文 M_Q を夫々、下記 (18), (19) と定義する。

$$M_P = g_1'' V_1^{(P)} + g_2'' V_2^{(P)} + \dots + g_{k+n}'' V_{k+n}^{(P)} \dots \quad (18)$$

$$M_Q = g_1'' V_1^{(Q)} + g_2'' V_2^{(Q)} + \dots + g_{k+n}'' V_{k+n}^{(Q)} \dots \quad (19)$$

【0068】

更に、素数P及び素数Qを、任意の拡大平文ベクトル g'' に対して $M_P < P$ かつ $M_Q < Q$ の条件を満たすように生成し、それらの積をNとする。中国人の剰余定理を用いて、P及びQによる余りが夫々 $V_1^{(P)}$ 及び $V_1^{(Q)}$ となるような最小の $V_1^{(N)} (< N)$ を導いて変換基數積と定義する。

【0069】

積和平文Mを、拡大平文ベクトル g'' と変換基數積 $V_1^{(N)}$ とを用いて、下記(20)のように定義する。ここで、 $M < N$ を満たす必要はない。

$$M = g_1'' V_1^{(N)} + g_2'' V_2^{(N)} + \dots + g_{k+n}'' V_{k+n}^{(N)} \dots \quad (20)$$

【0070】

Nより小さい乱数wを定め、下記(21)に従って、下記(22)に示すような公開鍵ベクトルcを導いて公開する。

$$c_i \equiv w V_i \pmod{N} \dots \quad (21)$$

$$\text{ベクトル } c = (c_1, c_2, \dots, c_{k+n}) \dots \quad (22)$$

【0071】

エンティティa側で、拡大平文ベクトル g'' と公開鍵ベクトルcとの内積を下記(23)のように求めて、暗号文Cを得る。作成された暗号文Cは通信路3を通してエンティティaからエンティティbへ送信される。なお、Nを公開する場合には、下記(23)のCをNで割った剰余を暗号文とすれば良い。

$$C = g_1'' c_1 + g_2'' c_2 + \dots + g_{k+n}'' c_{k+n} \dots \quad (23)$$

【0072】

エンティティb側では、以下のようにして復号処理が行われる。

積和平文Mは、下記(24)を満たす。従って、法P及び法Qにおける積和平文 M_P 及び M_Q は、下記(25), (26)のようにして求めることができる。

$$M \equiv w^{-1} C \pmod{N} \quad \dots \quad (24)$$

$$M_P \equiv M \pmod{P} \quad \dots \quad (25)$$

$$M_Q \equiv M \pmod{Q} \quad \dots \quad (26)$$

【0073】

拡大平文ベクトル g'' のうち、正規基数に対応するインデックス、即ち、 $i \in I$ に関しては、 $2^e < d_i^{(P)} d_i^{(Q)}$ であるため、下記 (27), (28) によつて $(g_i^{(P)}, g_i^{(Q)})$ を求め、中国人の剩余定理を適用することにより、下記 (29) が成立して、平文ベクトル g を復号することができる。

【0074】

【数5】

$$g_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \quad \dots \quad (27)$$

$$g_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \quad \dots \quad (28)$$

$$g_i \equiv \begin{cases} g_i^{(P)} \pmod{d_i^{(P)}} \\ g_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \quad \dots \quad (29)$$

【0075】

なお、退化基数に対応するインデックス、即ち、 $i \in I'$ に関しては、第1実施の形態と同様、復号する必要がなく、疑似平文ベクトル g' を正しく復号することができない。

【0076】

なお、上記例では、2組の基数 $\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$ に乱数 $\{v_i^{(P)}\}$, $\{v_i^{(Q)}\}$ を付加するようにしたが、このような乱数を付加しない基数積を使用しても良い。

【0077】

次に、上述したような第1, 第2実施の形態の方式にあって、LLLアルゴリズムに基づく低密度攻撃に強い耐性を持てるように、1を超える高い密度を実現できていることを説明する。退化していない一般的な積和型暗号について、暗号

文密度 σ ，方式密度 ρ ，レート η を下記 (30)，(31)，(32) のように定義する。なお、C は暗号文のビット数， C_{\max} は取り得る最大の暗号文のビット数，k は平文の分割数，e は分割平文のビット数である。

【0078】

【数6】

$$\sigma = \frac{\sum_{i=1}^k \log_2 g_i}{\log_2 C} \quad \dots \quad (30)$$

$$\rho = \frac{ke}{\log_2 C_{\max}} \quad \dots \quad (31)$$

$$\eta = \frac{ke}{|C_{\max}|} \quad \dots \quad (32)$$

【0079】

また、第1，第2実施の形態のように退化している積和型暗号について、暗号文密度 σ' ，方式密度 ρ' を下記 (33)，(34) のように定義する。なお、レートは上記 (32) と同じである。

【0080】

【数7】

$$\sigma' = \frac{\sum_{i=1}^{k+n} \log_2 g_i}{\log_2 C} \quad \dots \quad (33)$$

$$\rho' = \frac{(k+n)e}{\log_2 C_{\max}} \quad \dots \quad (34)$$

【0081】

第1実施の形態における密度について考察する。乱数 v_i を s ビットとする。

密度をできる限り大きくするために、取り得る最大の積和平文を M_{\max} とした場合、法 P のビットサイズを $|P| = |M_{\max}|$ と設定すべきである。この場合、第1実施の形態における方式密度 ρ_1 、レート η_1 は、夫々、下記 (35)、(36) の条件を満たす。

【0082】

【数8】

$$\begin{aligned} \rho_1 &= \frac{(k+n)e}{e + \log_2 P + \log_2 (k+n)} \\ &> \frac{(k+n)e}{(k+2)e + (n-1)e' + s + 2\log_2 (k+n) + 1} \\ &\dots \quad (35) \end{aligned}$$

$$\begin{aligned} \eta_1 &= \frac{ke}{e + \log_2 P + \log_2 (k+n)} \\ &> \frac{ke}{(k+2)e + (n-1)e' + s + 2\log_2 (k+n) + 1} \\ &\dots \quad (36) \end{aligned}$$

【0083】

公開鍵より秘密鍵を求める攻撃（片柳磨子、村上恭通、笠原正雄：“積和型暗号に関する二、三の考察”，1999年暗号と情報セキュリティシンポジウム資料，B43 Jan.2000 に開示）を回避するためには、乱数 v_i のビットサイズを法 P のビットサイズの $1/4$ 以上にする必要がある。この条件を満たすように、乱数 v_i のビットサイズを $s = (1/4)\log_2 P + 1$ と考えて計算した場合、方式密度 ρ_1 、レート η_1 は、夫々、下記 (37)、(38) の条件を満たす。

【0084】

【数9】

$$\rho_1 > \frac{3(k+n)e}{(4k+7)e + 4(n-1)e' + 7\log_2(k+n) + 7} \quad \dots \quad (37)$$

$$\eta_1 > \frac{3ke}{(4k+7)e + 4(n-1)e' + 7\log_2(k+n) + 7} \quad \dots \quad (38)$$

【0085】

この条件において、乱数 v_i が非常に大きいので、 e' を $e' < e/2$ とする
、または、 $k < n$ とすることにより、 $\rho_1 > 1$ を満たすパラメータが存在する。

【0086】

第2実施の形態における密度について考察する。乱数 $v_i^{(P)}$ と $v_i^{(Q)}$ との
積、即ち、 $v_i^{(P)} v_i^{(Q)}$ を s ビットとする。法Nが非公開である場合、密度
をできる限り大きくするために、取り得る最大の積和平文を $M_{P_{\max}}$, $M_{Q_{\max}}$ とし
たとき、 $|P| = |M_{P_{\max}}|$, $|Q| = |M_{Q_{\max}}|$ と設定すべきである。この場
合、第2実施の形態における方式密度 ρ_2 , レート η_2 は、夫々、下記 (39),
(40) の条件を満たす。

【0087】

【数10】

$$\begin{aligned} \rho_2 &= \frac{(k+n) e}{e + \log_2 N + \log_2 (k+n)} \\ &> \frac{(k+n) e}{(k+3)e + (n-1)e' + s + 3\log_2 (k+n) + 1} \\ &\dots \quad (39) \end{aligned}$$

$$\begin{aligned} \eta_2 &= \frac{k e}{e + \log_2 N + \log_2 (k+n)} \\ &> \frac{K e}{(k+3)e + (n-1)e' + s + 3\log_2 (k+n) + 1} \\ &\dots \quad (40) \end{aligned}$$

【0088】

第2実施の形態では、多重化しているので、乱数をあまり大きくする必要はない。よって、 $e' = e/2$, $k = n$ という条件であっても、容易に方式密度 $\rho_2 > 1$, レート $\eta_2 > 1/2$ を達成することができる。例えば、上記の条件において、分割数を $k = 8$ とし、基数 $d_i^{(P)}$, $d_i^{(Q)}$ 及び乱数 $v_i^{(P)}$, $v_i^{(Q)}$ を何れも32ビットとした場合、 $\rho_2 = 1.0174$, $\eta_2 = 0.5087$ となり、このような小さなパラメータでも、上記の条件 ($\rho_2 > 1$, $\eta_2 > 1/2$) を実現できている。但し、小さなパラメータでは安全性に問題があるので、例えば $k = 100$, $e = 64$, $e' = 32$ 程度が現実的である。

【0089】

また、法Nを公開とし、CをNで割った剰余を暗号文とした場合の第2実施の形態における方式密度 ρ_2 , レート η_2 は、夫々、下記 (41), (42) の条件を満たす。

【0090】

【数11】

$$\begin{aligned} \rho_2 &= \frac{(k+n) e}{\log_2 N} \\ &> \frac{(k+n) e}{(k+2)e + (n-1)e' + s + 2\log_2(k+n) + 1} \\ &\dots \quad (41) \end{aligned}$$

$$\begin{aligned} \eta_2 &= \frac{k e}{\log_2 N} \\ &> \frac{k e}{(k+2)e + (n-1)e' + s + 2\log_2(k+n) + 1} \\ &\dots \quad (42) \end{aligned}$$

【0091】

以上のように、法Nを公開とした場合には、法Nが非公開である場合に比べて、方式密度 ρ_2 、レート η_2 の何れもが向上している。

【0092】

ところで、疑似平文ベクトル g' における乱数成分は、平文ベクトル g とは全く独立して設定できる。よって、作成した暗号文Cの方式密度が高くなるように疑似平文ベクトル g' の乱数成分を設定するようにすれば良い。また、疑似平文ベクトル g' としてある乱数系列を設定して暗号文Cを作成した後、その暗号文Cの方式密度を計算し、その計算値が1を超えない場合には、疑似平文ベクトル g' に設定する乱数系列を別なものにして暗号文Cを作成しなおすようにし、方式密度が1を超えた場合の暗号文Cを受信先のエンティティへ送信する手法が有効である。

【0093】

上述した第1、第2実施の形態の方式では、エンティティ b へ特に暗号化して送信する必要がない疑似平文ベクトルの各乱数の拡大平文ベクトルにおける位置（退化位置）は受信側のエンティティ b にて固定的に設定されており、その位置

を表す情報が公開されている。

【0094】

これに対して、そのような乱数成分の位置（退化位置）、または逆に暗号化すべき平文ベクトルの各成分の位置（正規位置）を、任意に設定できるようすれば、より安全性が向上することを期待できる。以下の第3実施の形態では、このような退化位置または正規位置を受信側のエンティティaにて任意に設定して、その位置を表す情報を暗号文に盛り込んでエンティティbへ伝送する場合について説明する。

【0095】

(第3実施の形態)

まず、第3実施の形態の説明に用いる幾つかの定義について説明する。第3実施の形態にあっても、暗号化すべき平文は幾つかの分割平文に分けられる。各分割平文をメッセージベクトルmとして扱う。以下に定義する伸長変換によって、メッセージベクトルmはベクトルm'に伸長される。このベクトルm'を、伸長メッセージベクトルと称する。これらのベクトルm、ベクトルm'の各成分のビットサイズの和を夫々 ε （ビット）、 ε' （ビット）（但し、 $\varepsilon \leq \varepsilon'$ ）とする。また、暗号文が取り得る最大ビット数を C_{\max} とする。

【0096】

〈定義1（密度）〉

方式密度 ρ を下記(43)のように定義する。

【0097】

【数12】

$$\rho = \frac{\varepsilon'}{\log_2 C_{\max}} \quad \dots \quad (43)$$

【0098】

〈定義2（レート）〉

レート η を下記(44)のように定義する。

【0099】

【数13】

$$\eta = \frac{\epsilon}{|C_{\max}|} \quad \dots \quad (44)$$

【0100】

ベクトル $a = (a_1, a_2, \dots, a_w)$ を w 次元ベクトルとし、ベクトル $c = (c_1, c_2, \dots, c_n)$ を n 次元ベクトルとする。また、ベクトル $b = (b_1, b_2, \dots, b_n)$ を重み w の n 次元 2 値ベクトルとする。但し、下記 (45) の条件を満たす。

【0101】

【数14】

$$\left. \begin{array}{l} b_{i_1} = b_{i_2} = \dots = b_{i_w} = 1 \\ i_1 < i_2 < \dots < i_w \end{array} \right\} \dots \quad (45)$$

【0102】

<定義3 (添数集合)>

添数集合 $I = I \cap d$ (ベクトル b) を下記 (46) のように定義する。

$$I = \{i_1, i_2, \dots, i_w\} \quad \dots \quad (46)$$

【0103】

<定義4 (ベクトル表現)>

添数集合 I は、 $\{1, 2, \dots, n\}$ の部分集合であり、ベクトル表現として、ベクトル $d = Vec(I, n)$ を下記 (47) のように定義する。但し、ベクトル $d = (d_1, d_2, \dots, d_n)$ であり、例えば、 $I = I \cap d$ (ベクトル b) である場合に、ベクトル $b = Vec(I, n)$ である。

【0104】

【数15】

$$d_i = \begin{cases} 1 & (i \in I) \\ 0 & (i \notin I) \end{cases} \dots (47)$$

【0105】

<定義5(伸長)>

ベクトル b によりベクトル a から伸長された n 次元ベクトル c は、ベクトル $c = \text{ベクトル } a \{/ \text{ベクトル } b\}$ にて表記し、下記 (48) のように定義する。例えば、ベクトル $a = (a_1, a_2, a_3)$ 、ベクトル $b = (1, 0, 1, 1)$ である場合に、ベクトル $a \{/ \text{ベクトル } b\} = (a_1, 0, a_2, a_3)$ となる。

【0106】

【数16】

$$\begin{cases} c_{ij} = a_j \\ c_k = 0 \quad (b_k = 0 \text{ の場合}) \end{cases} \dots (48)$$

$$(j = 1, 2, \dots, w, k = 1, 2, \dots, n)$$

【0107】

<定義6(抜き出し)>

ベクトル b によりベクトル c から抜き出された w 次元ベクトル a は、ベクトル $a = \text{ベクトル } c \{/ \text{ベクトル } b\}$ にて表記し、下記 (49) のように定義する。例えば、ベクトル $c = (c_1, c_2, c_3, c_4)$ 、ベクトル $b = (1, 0, 1, 1)$ である場合に、第1、第3及び第4成分が抜き出されて、ベクトル $c \{/ \text{ベクトル } b\} = (c_1, c_3, c_4)$ となる。

【0108】

【数17】

$$\vec{a} = (c_{i_1}, c_{i_2}, \dots, c_{i_w}) \dots \quad (49)$$

【0109】

次に、第3実施の形態の具体的な方式について説明する。

<平文分割>

平文xは、 $e k$ ビットの複数のブロックに分割される。各ブロックは下記(50)のようにメッセージベクトルmで表現される。なお、 m_i ($i = 1, 2, \dots, k$) はeビットの整数である。

$$\text{ベクトル } m = (m_1, m_2, \dots, m_k) \dots \quad (50)$$

【0110】

<伸長変換>

メッセージベクトルmを、各成分がeビットの整数であるk次元ベクトルとし、乱数ベクトルrを、各成分が e' ビットの整数であるn次元ベクトルとする。但し、 $e < e'$ とする。また、ベクトルsを、重みkの($k + n$)次元の2値ベクトルとする。このベクトルsを「位置特定子」と称する。

【0111】

h を下記(51)のように設定し、ベクトル s' を $(h e - (k + n))$ ビットの任意の2値詰め物ベクトルとする。 $h e$ 次元の2値連接ベクトル[ベクトルs|ベクトル s']は、各成分がeビットの整数である下記(52)のようなh次元のベクトルtに分割できる。

【0112】

【数18】

$$h = \lceil (k+n) / e \rceil \dots \quad (51)$$

$$\vec{t} = (t_1, t_2, \dots, t_h) \dots \quad (52)$$

【0113】

$K = k + n + h$ とし、各添数集合 I_N , I_R 及び I_L を夫々下記 (53), (54) 及び (55) のように定義する。但し、バーベクトル s はベクトル s のビット補数を表す。

【0114】

【数19】

$$I_N = \text{Ind}(\overrightarrow{s}) \quad \dots \quad (53)$$

$$I_R = \text{Ind}(\overline{\overrightarrow{s}}) \quad \dots \quad (54)$$

$$I_L = \{k+n+1, k+n+2, \dots, K\} \quad \dots \quad (55)$$

【0115】

なお、上記例では添数集合 I_L の成分を最後尾の h 個としたが、これらの成分の位置は任意であって良い。このような場合、下記 (56), (57) の条件を満たし、ベクトル m' , ベクトル s は夫々下記 (58), (59) のように表される。

【0116】

【数20】

$$I_N \cup I_R \cup I_L = \{1, 2, \dots, K\} \quad \dots \quad (56)$$

$$I_N \cap I_R = I_R \cap I_L = I_L \cap I_N = \emptyset \quad \dots \quad (57)$$

$$\begin{aligned} \overrightarrow{m}' &= \overrightarrow{m} \{ \text{Vec}(I_N, K) \} + \\ &\quad \overrightarrow{r} \{ \text{Vec}(I_R, K) \} + \overrightarrow{t} \{ \text{Vec}(I_L, K) \} \quad \dots \quad (58) \end{aligned}$$

$$\overrightarrow{s} = \text{Vec}(I_N, K) [\overline{\text{Vec}(I_L, K)}] \quad \dots \quad (59)$$

【0117】

メッセージベクトル m を、下記 (60) のように、伸長メッセージベクトル $m' = (m_1', m_2', \dots, m_K')$ に変換する。この際、このベクトル m' の各成分の大きさは下記 (61) である。

【0118】

【数21】

$$\vec{m} = [\vec{m} \ (\vec{s}) + \vec{r} \ (\overline{\vec{s}}) | \vec{t}] \ \cdots \ (60)$$

$$|m_i'| = \begin{cases} e & (i \in I_N \cup I_L) \\ e' & (i \in I_R) \end{cases} \ \cdots \ (61)$$

【0119】

<鍵生成>

秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵: $\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$, $\{v_i^{(P)}\}$, $\{v_i^{(Q)}\}$,
 P, Q, N, w (但し、 $i = 1, 2, \dots, K$)
- ・公開鍵: ベクトル $c = (c_1, c_2, \dots, c_K)$, I_L , e , e'

なお、上記Nは公開であっても良い。

【0120】

まず、任意の i, j (但し、 $i \neq j$)について、下記 (62) ~ (65) の条件を満たすような2組の基數 $\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$ を生成する。

【0121】

【数22】

$$\gcd(d_i^{(P)}, d_j^{(P)}) = 1 \ \cdots \ (62)$$

$$\gcd(d_i^{(Q)}, d_j^{(Q)}) = 1 \ \cdots \ (63)$$

$$\gcd(d_i^{(P)}, d_i^{(Q)}) = 1 \ \cdots \ (64)$$

$$d_i^{(P)} d_i^{(Q)} = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \ \cdots \ (65)$$

【0122】

$v_i^{(P)}$, $v_i^{(Q)}$ をランダムな整数として、下記 (66), (67) のように、
 $v_i^{(P)}$, $v_i^{(Q)}$ を導く。但し、 $v_i^{(P)}$ 及び $v_i^{(Q)}$ は、下記 (68) 及び (69) の条件を満たす。

【0123】

【数23】

$$V_i^{(P)} = \frac{d_1^{(P)} d_2^{(P)} \cdots d_k^{(P)}}{d_i^{(P)}} v_i^{(P)} \quad \dots \quad (66)$$

$$V_i^{(Q)} = \frac{d_1^{(Q)} d_2^{(Q)} \cdots d_k^{(Q)}}{d_i^{(Q)}} v_i^{(Q)} \quad \dots \quad (67)$$

$$\gcd(d_i^{(P)}, v_i^{(P)}) = 1 \quad \dots \quad (68)$$

$$\gcd(d_i^{(Q)}, v_i^{(Q)}) = 1 \quad \dots \quad (69)$$

【0124】

次に、任意の伸長メッセージベクトル m' について条件 $M_P < P$, $M_Q < Q$ を満たすような大きな素数 P , Q を設定する。なお、 M_P , M_Q は夫々下記 (70), (71) で定義される。

【0125】

【数24】

$$M_P = m'_1 V_1^{(P)} + m'_2 V_2^{(P)} + \cdots + m'_K V_K^{(P)} \quad \dots \quad (70)$$

$$M_Q = m'_1 V_1^{(Q)} + m'_2 V_2^{(Q)} + \cdots + m'_K V_K^{(Q)} \quad \dots \quad (71)$$

【0126】

そして、 $N = P Q$ を設定し、中国人の剰余定理により V_i ($0 \leq V_i < N$) を下記 (72) により計算する。

【0127】

【数25】

$$V_i \equiv \begin{cases} V_i^{(P)} \pmod{P} \\ V_i^{(Q)} \pmod{Q} \end{cases} \quad \dots \quad (72)$$

【0128】

公開鍵ベクトル c の各成分を、下記 (73) により求める。ここで w は、 Z_N^* から任意に選ばれた乱数である。

$$c_i \equiv w V_i \pmod{N} \quad \dots (73)$$

【0129】

〈暗号化〉

エンティティ a 側（送信側）で、前述した位置特定子であるベクトル s を任意に生成する。即ち、メッセージベクトル m に関する位置を示す添数集合 I_N を、送信者であるエンティティ a は任意に選択する。次に、エンティティ a 側（送信側）で、各成分が任意に選択された e' ビットの整数からなる n 次元のベクトル r を生成する。この乱数ベクトル r により、高密度が実現される。つまり、冗長部分（退化部分）である乱数ベクトル r の付加によって、後述するように密度が高くなる。

【0130】

エンティティ a 側（送信側）で、メッセージベクトル m を、ベクトル s 及びベクトル r によって、伸長メッセージベクトル m' に変換する。そして、この伸長メッセージベクトル m' と公開鍵ベクトル c との内積を下記 (74) のように求めて、暗号文 C を得る。作成された暗号文 C は通信路 3 を介してエンティティ a からエンティティ b へ送信される。

【0131】

【数26】

$$\begin{aligned} C &= \vec{m'} \cdot \vec{c} \\ &= m'_1 c_1 + m'_2 c_2 + \cdots + m'_K c_K \quad \dots (74) \end{aligned}$$

【0132】

この暗号化にあっては、暗号化すべき平文を分割したメッセージベクトル m は、添数集合 I_N にて示される位置で伝送され、添数集合 I_N の情報は、添数集合 I_L にて示される位置でベクトル s によって伝送される。

【0133】

〈復号〉

エンティティ b 側（受信側）で、以下のようにして復号処理が行われる。

中間メッセージ M は、下記 (75) を満たす。従って、法 P, 法 Q における中間メッセージ M_P, M_Q は、下記 (76), (77) のようにして求めることができる

$$M \equiv w^{-1} C \pmod{N} \quad \dots (75)$$

$$M_P \equiv M \pmod{P} \quad \dots (76)$$

$$M_Q \equiv M \pmod{Q} \quad \dots (77)$$

【0134】

そして、下記 (78), (79) によって $(m_i^{(P)}, m_i^{(Q)})$ を求め、中国人の剩余定理を適用することにより、下記 (80) が成立して、メッセージベクトル $m'' = (m_1'', m_2'', \dots, m_k'')$ を復号することができる。

【0135】

【数27】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d; (P)} \quad \dots (78)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d; (Q)} \quad \dots (79)$$

$$m_i'' \equiv \begin{cases} m_i^{(P)} & \pmod{d; (P)} \\ m_i^{(Q)} & \pmod{d; (Q)} \end{cases} \quad \dots (80)$$

【0136】

$e' > e$ であるので、復号されたメッセージベクトル m'' の各成分は、上記 (61) から、下記 (81) の条件を満たす。

【0137】

【数28】

$$\begin{cases} m_i'' = m_i' & (i \in I_N \cup I_L) \\ m_i'' \neq m_i' & (i \in I_R) \end{cases} \dots (81)$$

【0138】

添数集合 I_L に従って、下記 (82) のように、復号ベクトル m'' からベクトル t を取り出す。

【0139】

【数29】

$$\vec{t} = \vec{m}'' [\text{Vec}(I_L, K)] \dots (82)$$

【0140】

ベクトル t を $h \times e$ 次元の2値ベクトル [ベクトル s | ベクトル s'] と見なすことにより、 $(k+n)$ 次元で重み k の2値ベクトル s をエンティティ b 側（受信側）で再構築できる。よって、最終的に、下記 (83) のように、メッセージベクトル m を得ることができる。

【0141】

【数30】

$$\vec{m} = \vec{m}'' [\vec{s}] \dots (83)$$

【0142】

なお、添数集合 I_L の成分を任意とする一般的な場合には、上記 (83) において、ベクトル m'' を下記 (84) に示すものに代えることにより、メッセージベクトル m が得られる。

【0143】

【数31】

$$\vec{m}'' [\overline{\text{Vec}(I_L, K)}] \dots (84)$$

【0144】

次に、上述したような第3実施の形態の暗号化方式における安全性について述べる。密度が0.9408より小さい場合に、積和型公開鍵暗号はLLLアルゴリズムに基づく低密度攻撃によって破られることが知られている。上述した第3実施の形態の暗号化方式では、1を超える高い密度を実現できており、このことはこの方式が低密度攻撃に対して安全であることを示している。

【0145】

乱数 $v_i^{(P)}, v_i^{(Q)}$ を何れも f ビットとした場合、上述した第3実施の形態の暗号化方式における密度 ρ は、下記 (85) の条件を満たす。但し、 $K = k + n + h, e' > e$ である。

【0146】

【数32】

$$\begin{aligned} \rho &> \frac{(k+h)e+ne'}{e'+\log_2 N+\log_2 n} \\ &> \frac{Ke+n(e'-e)}{Ke+(3e'-e)+f+1+3\log_2 n} \quad \dots \quad (85) \end{aligned}$$

【0147】

例えば、ここで簡単のために、 $f = e, e' = 2e$ と設定した場合、 n は下記 (86) の条件を満たすので、 $\rho > 1$ を実現できている。現実的な例として、 $e = 32$ とした場合、何れの k についても $n = 7$ とすることにより、 $\rho > 1$ を達成できることが分かる。

【0148】

【数33】

$$(n-6)e > 3\log_2 n + 1 \quad \dots \quad (86)$$

【0149】

また、第3実施の形態の暗号化方式では、高いレートも実現できている。上述した本発明の暗号化方式におけるレート η は、下記 (87) の条件を満たす。

【0150】

【数34】

$$\begin{aligned}\eta &= \frac{ke}{e' + \log_2 N + \log_2 n} \\ &> \frac{ke}{Ke + (3e' - e) + f + 1 + 3\log_2 n} \quad \dots \quad (87)\end{aligned}$$

【0151】

ここで簡単のために、 $f = e$, $e' = 2e$ と設定した場合、 n 及び k は下記(88)の条件を満たすので、 $\eta > 0.5$ を実現できている。現実的な例として、 $e = 32$ とした場合、 $n = 7$ で $k > 14$ とすることにより、 $\eta > 0.5$ を達成できることが分かる。例えば、 $k = 57$ とした場合に、 $\eta = 0.7884$ となる。このように、レートの観点から見ても、第3実施の形態の方式は効率的である。

【0152】

【数35】

$$\left(k - n - \left\lceil \frac{k+n}{e} \right\rceil - 6\right)e > 3\log_2 n + 1 \quad \dots \quad (88)$$

【0153】

第3実施の形態の暗号化方式では、高い密度を実現できるため、低密度攻撃に対し、十分に安全である。また、送信側のエンティティにおいて、退化基數の位置を自由に決定できる。よって、位置が分かっている退化基數に基づき、攻撃者が第3実施の形態の暗号化方式に対して有効な攻撃を行おうとした場合でも、その攻撃者にとって退化基數の位置を同定することが困難である。従って、退化基數の位置が固定ではなく送信側で任意に決定できるという第3実施の形態の特徴は、退化基數の位置が既知である場合に有効である攻撃に対しても安全であることを示している。

【0154】

以下、第3実施の形態の他の例について説明する。上述した例では全てのプロ

ックにおいて、 I_L の位置を固定（最後尾）としているが、この I_L の位置は各ブロックにおいて異なっていても良い。このような例として、以下のようなものが可能である。

【0155】

(第1例)

最初のブロックについては I_L の位置を固定（例えば上述した例と同様に最後尾）し、この I_L は公開しておく。そして、2番目以降のブロックについては、1つ前のブロックのメッセージベクトルよりそのブロックの I_L の位置を決定するようとする。よって、2番目以降のブロックからは、 I_L の位置が変動する。このようにして、送信側のエンティティが退化基数の位置を任意に決定しても最初のブロックの I_L は公開されており、しかも、2番目以降のブロックでは前のブロックのメッセージベクトルからそのブロックの I_L の位置が分かるので、受信側のエンティティにおいて、上述した例と同様に、暗号文から平文を復号できる。この第1例では、各ブロックにおいて I_L の位置を変動させるため、安全性の向上を図れる。

【0156】

(第2例)

最初のブロックについては I_L の位置を固定（例えば上述した例と同様に最後尾）し、この I_L は公開しておく。そして、2番目以降のブロックについては、 I_L の項を設けないようにし、 I_L の項に割り当てられる h 次元のベクトルを平文を分割したメッセージに割り当てる。そして、この2番目以降のブロックについては、1つ前のブロックのメッセージよりそのブロックにおける退化基数の位置を示す位置情報を決定する。よって、2番目以降のブロックには、 I_L が存在しない。このようにして、送信側のエンティティが退化基数の位置を任意に決定しても最初のブロックの I_L は公開されており、しかも、2番目以降のブロックでは前のブロックのメッセージベクトルからそのブロックでの退化基数の位置が分かるので、受信側のエンティティにおいて、上述した例と同様に、暗号文から平文を復号できる。また、2番目以降のブロックではメッセージに割り当てる部分が k 項から $(k + h)$ 項に増えるので、1ブロック内に盛り込めるメッセージ

量が増加して、レートをより高くすることができる。

【0157】

なお、上記例では、暗号化すべき平文を分割したメッセージベクトルmの各成分の位置（添数集合 I_N ）を示す情報（添数集合 I_L ）を伝送するようにしたが、付加する乱数ベクトルrの各成分の位置（添数集合 I_R ）を示す情報を伝送するようにしても良いことは勿論である。

【0158】

また、上記例では、2組の基底 $\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$ に乱数 $\{v_i^{(P)}\}$, $\{v_i^{(Q)}\}$ を付加するようにしたが、このような乱数を付加しない基底積を使用しても良い。

【0159】

また、上記例では(74)に示したように、伸長メッセージベクトル m' と公開鍵ベクトルcとの内積値（積和演算結果）をそのまま暗号文Cとしたが、下記(89)のように、その内積値（積和演算結果）をNでモジュロ変換したもの、つまり上記(74)のCをNで割った剰余を暗号文としても良い。

$$C \equiv m_1' c_1 + m_2' c_2 + \cdots + m_K' c_K \pmod{N} \quad \cdots (89)$$

【0160】

(74)のように暗号文を表す場合に、安全性の根拠は、下記(90)に示す式において、 a_1, a_2, \dots, a_n 及びCが既知の整数であるときに未知数 x_1, x_2, \dots, x_n を求めるための線型ジオファンタス方程式を解くことの困難さに基づいている。一方、(89)のように暗号文を表す場合には、積和してモジュロをとるので、安全性の根拠がNの素因数分解の困難さに基づいている。この場合、Nを公開するので攻撃者に提供する情報量は増えるが、積和演算結果そのものではなくてその余りしか分からないので、線型ジオファンタス方程式を解く難しさは高くなっている。

$$C = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \quad \cdots (90)$$

【0161】

(第4実施の形態)

なお、第3実施の形態では、送信側のエンティティにて任意に設定した、伸長

メッセージベクトルにおけるメッセージベクトルの各成分または乱数ベクトルの各成分の位置を示す情報を暗号文に盛り込むようにしたが、このような位置を示す情報を、暗号文との伝送とは独立させて、送信側のエンティティから受信側のエンティティへ報せるようにしても良い。

【0162】

(第5実施の形態)

なお、第3、第4実施の形態では、送信側のエンティティにて伸長メッセージベクトルにおけるメッセージベクトルの各成分または乱数ベクトルの各成分の位置を任意に設定するようにしたが、このような位置を受信側のエンティティにて任意に設定するようにすることも可能である。

【0163】

(第6実施の形態)

また、第3～第5実施の形態では、K個の要素からなる基底の集合 $\{d_i\}$ を2組 ($\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$) 生成する多重化した方式の場合について説明したが、前述した第1実施の形態のように1組の基底の集合 $\{d_i\}$ を用いる方式についても、これらの第3～第5実施の形態を同様に適用できることは勿論である。

【0164】

図2は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するコンピュータプログラムは、上述した暗号化方式の手順に従って拡大平文ベクトル g'' または伸長メッセージベクトル m' を得る処理と、得た拡大平文ベクトル g'' または伸長メッセージベクトル m' と公開鍵ベクトル c との内積計算により暗号文 C を作成する処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ10は、送信側のエンティティに設けられている。

【0165】

図2において、コンピュータ10とオンライン接続する記録媒体11は、コンピュータ10の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体11には前述の如きプログラム11aが記録されている。記録媒体11から通信線等の伝送媒体14を介して読み出されたプログ

ラム11a がコンピュータ10を制御することにより、コンピュータ10が暗号文Cを作成する。

【0166】

コンピュータ10の内部に設けられた記録媒体12は、内蔵設置される例えばハードディスクドライブまたはROMなどを用いてなり、記録媒体12には前述の如きプログラム12a が記録されている。記録媒体12から読み出されたプログラム12a がコンピュータ10を制御することにより、コンピュータ10が暗号文Cを作成する。

【0167】

コンピュータ10に設けられたディスクドライブ10a に装填して使用される記録媒体13は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキシブルディスクなどを用いてなり、記録媒体13には前述の如きプログラム13a が記録されている。記録媒体13から読み出されたプログラム13a がコンピュータ10を制御することにより、コンピュータ10が暗号文Cを作成する。

【0168】

【発明の効果】

以上のように、本発明では、暗号化すべき平文を分割してなる平文ベクトルに、複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルと、公開されている公開ベクトルとを用いて暗号文を得るようにしたので、暗号化が必要でない乱数からなる冗長部分（退化部分）を付加しているため、暗号文の密度を大きくでき、LLLアルゴリズムに基づく低密度攻撃に対して強くなつて安全性を向上できる。また、その合成ベクトルにおける平文ベクトルまたは乱数ベクトルの各成分の位置を、送信側のエンティティまたは受信側のエンティティにて任意設定できるようにしたので、攻撃者にとってその位置を見つけることすら困難であり、安全性の更なる向上を図れる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図1】

2人のエンティティ間における情報の通信状態を示す模式図である。

【図2】

記録媒体の実施の形態の構成を示す図である。

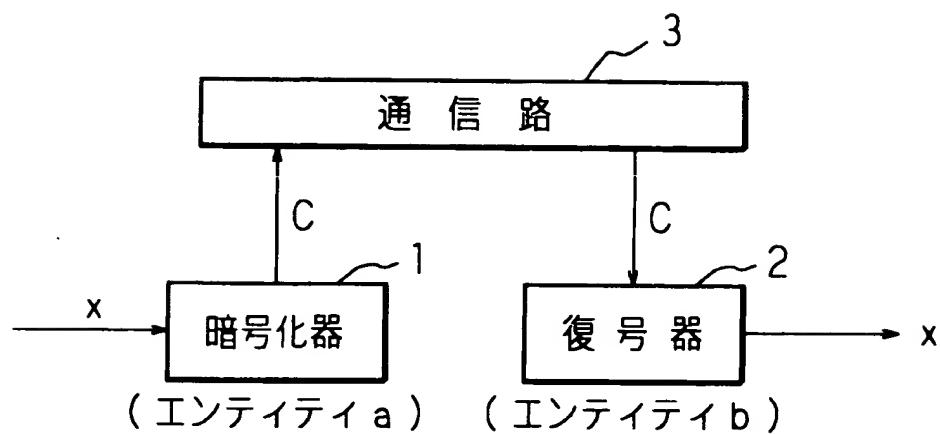
【符号の説明】

- 1 暗号化器
- 2 復号器
- 3 通信路

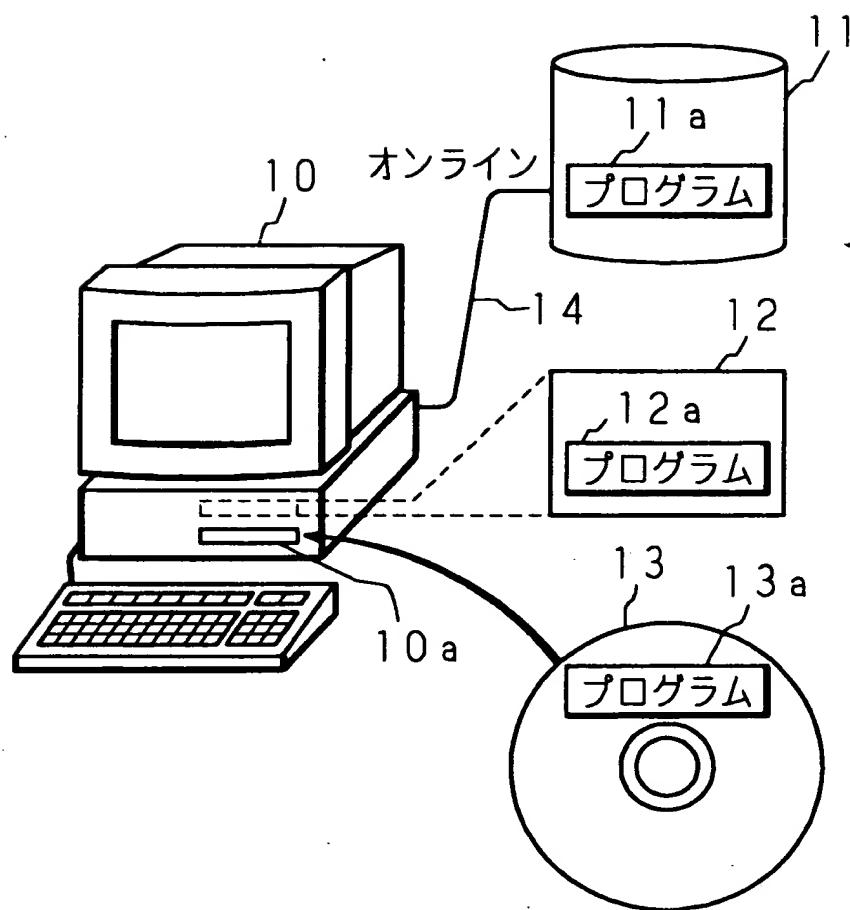
a, b エンティティ

【書類名】 図面

【図1】



【図2】



【書類名】 要約書

【要約】

【課題】 LLLアルゴリズムに基づく低密度攻撃に強く、安全性を向上できる暗号化方式を提供する。

【解決手段】 暗号化すべき平文を分割した平文ベクトルに任意の乱数成分からなる乱数ベクトルを加えた合成ベクトルの各成分と、1または複数組の整数 d_i ($1 \leq i \leq K$) 及び乱数 v_i を用いて $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_K$ (任意の2つの整数 d_i, d_j は互いに素)) に設定された1または複数の基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文 C を得る。合成ベクトルにおける平文ベクトルまたは乱数ベクトルの各成分の位置は、送信側 (エンティティ a) または受信側 (エンティティ b) で任意に設定する。

【選択図】 図 1

出願人履歴情報

識別番号 [000006297]

1. 変更年月日 1990年 8月 7日

[変更理由] 新規登録

住 所 京都府京都市南区吉祥院南落合町3番地
氏 名 村田機械株式会社

出願人履歴情報

識別番号 [597008636]

1. 変更年月日 1997年 1月21日

[変更理由] 新規登録

住 所 大阪府箕面市粟生外院4丁目15番3号
氏 名 笠原 正雄